REMARKS/ARGUMENTS

Claims 1-45 are pending in the present application. Claims 1-5, 10, 16-20, 25, 31-35 and 40 have been amended herewith. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 102, Anticipation

Claims 1, 2, 6-17, 21-32 and 36-45 stand rejected under 35 U.S.C. § 102 as being anticipated by Yavatkar et al. (U.S. Patent No. 6,735,702), hereinafter "Yavatkar". This rejection is respectfully traversed.

Generally, Claim 1 is directed to techniques for mitigating, through the claimed monitoring/identifying/altering steps, detrimental network conditions that may exist within a distributed data processing system. Specifically, packets having certain small size characteristics can be detrimental to a network because of the overhead associated with packet transfer is typically fairly the same amount of overhead irrespective of the packet size (Specification page 5, line 28 – page 6, line 9). Thus, the percentage of network resources required for processing relatively small packets is substantially greater than the percentage of network resources required for processing relatively large packets. The present invention as provided by Claim 1 is able to identify such detrimental small size packet criteria and take appropriate action in response thereto. In contrast, per the teachings of the cited Yavatkar reference, the *number of overall packets* is tracked to determine if the quantity of overall packets exceeds some safety criteria. Quite simply, identifying individual packet sizes is very different from identifying an overall quantity of packets.

A simple analogy will further establish this fundamental difference. Many large cities have freeway carpool lanes where the lanes can only be used for automobiles having more than a minimum number of occupants. For example, some carpool lanes may be restricted to automobiles having more than one passenger. Claim 1 is akin to monitoring occupants in automobiles in a carpool lane to ensure that the minimum number of occupants is being met. In contrast, the teachings of the cited Yavatkar reference are more akin to counting the total number of automobiles in a carpool lane, with no determination being made as to the actual number of occupants in any of the automobiles[1]. Counting the number of automobiles in a carpool line provides no information with respect to the number of occupants in the automobiles. Thus, a teaching of determining a total amount of traffic in a network (as per the

[1] This automobile carpool lane analogy is very similar to the present claims, as the purpose of the carpool lanes is to deter single passenger automobiles as the overhead associated with their automobile – space taken on the highway, amount of generated pollution, etc. – is essentially the same irrespective of the number of occupants in the car, and thus the more occupants there are in the individual automobiles, the more efficient the highway operates (and thus this analogy example is extremely relevant to a data network environment, with a desire to reduce the number of relatively small packets to similarly mitigate associated undesirable packet processing overhead).

teachings of the cited reference) does not inherently teach any determination being made with respect to individual packet sizes for packets in such network.

Claim 1 has been amended to directly tie-in the packet size as being the critical criteria that is used in the claimed identifying step. As amended, Claim 1 recites "identifying a source of network packets as generating network packets having packet size characteristics directly related to packet size of individual packets of the network packets that satisfy one or more predetermined conditions". As can be seen, the source of network packets having *particular* <u>*packet size*</u> *characteristics is identified.* In rejecting the 'identifying' step of Claim 1, the Examiner cites Yavatkar description at col. 1, lines 55-67 and col. 1, lines 65-67 through col. 2, lines 1-45 as teaching such identifying step. Applicants urge that there, Yavatkar states:

> The source of attacks may be difficult to diagnose due to the nature of typical network architecture and due to subterfuge methods an attacking machine may use. While normally a network packet identifies the sender of the packet, a device sending hostile messages may disguise this through IP spoofing, where a false source IP address is inserted in sent packets. In addition, on a network having multiple gateways to other networks, it may not be readily apparent which of the multiple gateways is allowing a flood of hostile messages to enter the network.
>
> Systems exist for *collecting information about network traffic*. For example, to determine the node which is the *source of attack* <u>*traffic*</u> (or the gateway allowing such traffic into a network, which in such a case may be considered a source) and the path or paths taken by such traffic, a human operator may access each link at a node receiving such traffic and *analyze the incoming* <u>*traffic*</u> using a sniffer. A sniffer is a device which may record network statistics at a node. The operator may identify *which of the physical links attached to the node is receiving a certain type or* <u>***amount***</u> <u>*of traffic*</u> and then move to the node on the other end of the identified link. The path or paths of traffic from the source of the traffic may be found by traversing the network from node to node, using the sniffer at each node in a path, until the source is reached. Such a diagnosis is slow and inaccurate. A similar analysis may be performed from a central console which may query remote nodes for information about the source of incoming traffic. Such a diagnosis is also slow and inaccurate, as it requires commands to nodes and responses from nodes to be transmitted across the network. The speed at which attacks occur and the speed at which such problems must be fixed makes such detection methods ineffective. *A path taken by* <u>*traffic*</u> may be described as the equipment traversed by traffic as the traffic crosses a network or networks (e.g., a series of nodes and links, or a series of sub-networks).
>
> Diagnosing network attacks may thus require the distributed state of the network to be known--e.g., *what type of* <u>*traffic*</u> *is being received at which devices and through which ports, and the path or paths taken by the* <u>*traffic*</u>. Certain information about the state of a network may only be gathered accurately and quickly at the individual nodes distributed throughout a network--for example, the *particular port receiving a certain type of attack* <u>*traffic*</u>. Currently, gathering such information requires that an operator physically access individual nodes, e.g., by using a sniffer, or that a central console query remote nodes. Such methods are slow, inefficient and inaccurate. The time taken to perform current

> diagnosis operations results in inaccuracy, as the state of a network is determined over a period of time. Delays may also occur, if (as may happen during a network attack), data transmission over links is interrupted or halted. The state of a network is not always accurately viewed from one central point which has only indirect access to the state of remote network nodes. Evidence of the source of attack traffic exists with greater certainty nearer *the source of the <u>traffic</u>.*

As can be seen, the cited Yavatkar reference describes determining network traffic, but does not describe any type of packet size determination being made as a part of such traffic analysis. As previously described, monitoring of network traffic does not inherent teach any determination being made with respect to individual packet *sizes*, but instead describes determining the *number* of packets. It is urged that the amendment to Claim 1 has further emphasized this critical distinction. In addition, because there is no *inversely proportionally* relationship between the amount of Yavatkar overhead traffic and overhead associated with such traffic (instead, there is a *proportional* relationship – the more traffic, the more overhead), the resulting advantages provided by Claim 1 of improving networking efficiency by mitigating unwanted overhead is similarly not achieved by the teachings of the cited reference. Instead, the network offender is identified and blocked. Thus, it is urged that amended Claim 1 is not anticipated by the cited reference.

Applicants initially traverse the rejection of Claims 2 and 6-15 for similar reasons to those given above with respect to Claim 1.

Further with respect to Claim 2, such claim recites "wherein a predetermined condition of the one or more predetermined conditions is a packet size less than a predetermined packet size threshold value". As can be seen, Claim 2 expressly recites use of a packet size threshold value. In rejecting Claim 2, the Examiner states that this claimed feature is inherent in the teachings of the cited reference since the cited reference describes nodes that can store files. Applicants urge that the storing of a file in a node is equivalent to storing a file on a hard disk of a computer. Such storage of a file to a storage medium does not inherently teach packets sizes or associated packet size thresholds for *network packets*. Rather, such assertion is directed to internal operations <u>*within*</u> *a given node*. This can also be seen by the teachings of the cited reference at col. 7, lines 13-15 with reference to Figure 1, where it states:

> "Network communications device 130 allows node 30 to connect to network 4 via links 88, 90, 92, 94, and 96"

As can be seen, operations within a node, such as storing a file, do not teach <u>*network*</u> *packets*. Thus, it is urged that an allegation that it is inherent to store files within a node does not establish any teaching – either expressly or inherently – with respect to network packet sizes and associated thresholds, as recited in Claim 2. Thus, it is further urged that Claim 2 is not anticipated by the cited reference.

Further with respect to Claim 10 (and dependent Claims 11-15), Applicants have amended such claim in accordance with the Specification description at page 46, lines 11-20. Claim 10 is specifically directed to distributed packet snoopers and associated packet filters that are used in matching packets that meet the criteria designated by such filters. In rejecting Claim 10, the Examiner states that the cited reference teaches the receiving of a packet filter at a packet snooper since the cited reference describes the use of agents to collect information at col. 4, lines 24-30. Applicants respectfully urge that 'usage' of agents does not describe any type of filter being received by such agents. In fact, as stated in the several sentences immediately following this cited passage, the reference states:

> *Mobile agents may determine, <u>without exchanging</u> information or commands from a central location or human operator*, which path to take to further investigate an attack. *Since communication between a central console and a remote node is <u>not required</u>*, a finer granularity of information may be collected and acted upon. Accuracy is improved by the speed at which agents may gather, process, and act on information

Thus, the cited reference expressly teaches away from the features of Claim 10 (and dependent Claims 11-14) due to the desire to *maintain agent <u>autonomy</u>* to improve information collection. Thus, it is further urged that Claim 10 is not anticipated by the cited reference.

Further with respect to Claim 15, such claim recites "displaying the identified source of network packets to the system administrator in real time". In rejecting Claim 15, the Examiner states that the cited reference teaches this claimed displaying step since:

> "it is known that the computer network communication within the WAN and LAN using PC, Laptop or Workstation via TCP/IP is running in the real time to transport information, refer to Col. 1, Lines 10-35"

Applicants urge that even assuming arguendo that the above statement is true, such assertion does not establish any teaching by the cited reference of the claimed feature of "displaying *the identified source* of network packets *to the system administrator in real time*". Instead, such assertion merely establishes that information is *<u>transported</u> in real time*. Claim 1 is directed to *<u>displaying</u> information in real time* – with such displayed information being the *<u>identified source</u> of network packets*. Thus, it is further urged that Claim 15 is not anticipated by the cited reference, as there are additional claimed features that are not taught by the cited reference.

Applicants traverse the rejection of Claims 16, 17, 21-32 and 36-45 for similar reasons to those given above with respect to Claim 1.

Applicants further traverse the rejection of Claims 17 and 32 for similar reasons to the further reasons given above with respect to Claim 2.

Applicants further traverse the rejection of Claims 25 (and dependent Claims 26-29) and 40 (and dependent Claims 41-44) for similar reasons to the further reasons given above with respect to Claim 10.

Applicants further traverse the rejection of Claims 30 and 45 for similar reasons to the further reasons given above with respect to Claim 15.

Therefore, the rejection of Claims 1, 2, 6-17, 21-32 and 36-45 under 35 U.S.C. § 102 has been overcome.

II. 35 U.S.C. § 103, Obviousness

Claims 3-5, 18-20 and 33-35 stand rejected under 35 U.S.C. § 103 as being unpatentable over Yavatkar et al. (U.S. Patent No. 6,735,702), hereinafter "Yavatkar" in view of Mawhinney et al. (U.S. Patent No. 6,826,620), hereinafter "Mawhinney". This rejection is respectfully traversed.

Applicants initially traverse the reject of Claims 3-5 (and similarly for Claims 18-20 and 33-35) for similar reasons to those given above with respect to Claim 1, as the newly cited reference to Mawhinney does not overcome the teaching deficiency identified hereinabove.

Further with respect to Claim 3 (and similarly for Claims 18 and 33), such claim recites "wherein a predetermined condition is a computed percentage value of an actual packet payload size in comparison to a maximum available packet payload size". As can be seen, the predetermined condition of Claim 1 is defined per Claim 3 to be a computed percentage value, with the two parameters used for such computed percentage being (i) actual packet payload size and (ii) maximum available packet payload size. In rejecting Claim 3, the Examiner acknowledges that the cited Yavatkar reference does not teach such a computed percentage value. However, the Examiner alleges that the cited Mawhinney reference teaches such computed percentage value with respect to packet payload sizes at col. 3, lines 30-35 since such passage describes 'percentage of network availability". Applicants show that there, Mawhinney states:

> "This level of service can be measured by, for example, network availability as a percentage of total time on the network, the amount of data actually delivered through the network compared to the amount of data attempted, or possibly the network latency, or the amount of time it takes for a particular communication to traverse the network."

This cited passage describes various parameters that can be used to define a particular level of service, including (i) percentage of *total time* on the network, (ii) amount of data delivered versus amount of data attempted to be delivered, (iii) network latency (which is *time-based*), (iv) amount of *time* it takes to traverse the network. As can be seen, three of these four criteria pertaining to a service level are based on *time*, and not on packet *size*. The only quantifiable parameter associated with an amount of data (per this cited reference) is an amount of data delivered versus an amount of data attempted. In contrast, per

the features of Claim 3 it is *packet* <u>*payload sizes*</u> (actual and maximum). Thus, it is urged that Claim 3 (and similarly for Claims 18 and 33) has been erroneously rejected as the Examiner has failed to properly establish a prima facie showing of obviousness with respect to such claim – as none of the cited references teach or otherwise describe packet payload sizes being used as criteria pertaining to the predetermined condition (which is used in the identifying step of Claim 1).

Applicants further traverse the rejection of Claims 4, 5, 19, 20, 34 and 35 for similar reasons to the further reasons given above with respect to Claims 3, 18 and 33 and the missing packet size features.

Therefore, the rejection of Claims 3-5, 18-20 and 33-35 under 35 U.S.C. § 103 has been overcome.

III. <u>Conclusion</u>

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: <u>November 15, 2007</u>

Respectfully submitted,

<u>/Wayne P. Bailey/</u>

Wayne P. Bailey
Reg. No. 34,289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants